



***Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy***



070.110 Technology Acquisition

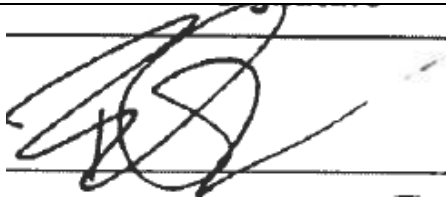
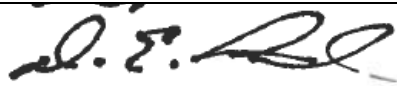
**Version 2.3
February 19, 2018**

070.110 Technology Acquisition	Current Version: 2.3
070.000 Administrative	Review Date: 02/19/2018

Revision History

Date	Version	Description	Author
7/30/2013	1.0	Effective Date	CHFS IT Policies Team Charter
2/19/2018	2.3	Revision Date	CHFS OATS Policy Charter Team
2/19/2018	2.3	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
IT Executive, Office of the Secretary (or designee)	2/19/2018	<u>Bernard "Deck" Decker</u>	
CHFS Chief Security Officer (or designee)	2/19/2018	DENNIS E. LEBER	

070.110 Technology Acquisition	Current Version: 2.3
070.000 Administrative	Review Date: 02/19/2018

Table of Contents

070.110 TECHNOLOGY ACQUISITION	5
1 POLICY OVERVIEW.....	5
1.1 PURPOSE	5
1.2 SCOPE	5
1.3 MANAGEMENT COMMITMENT.....	5
1.4 COORDINATION AMONG ORGANIZATIONAL ENTITIES	5
1.5 COMPLIANCE	5
2 ROLES AND RESPONSIBILITIES	6
2.1 CHIEF INFORMATION SECURITY OFFICER (CISO)	6
2.2 SECURITY/PRIVACY LEAD	6
2.3 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY OFFICER	6
2.4 CHFS STAFF AND CONTRACT EMPLOYEES	6
3 POLICY REQUIREMENTS	7
3.1 REGULATIONS.....	7
3.2 POLICY VIOLATIONS	7
4 POLICY MAINTENANCE RESPONSIBILITY	7
5 POLICY EXCEPTIONS	7
6 POLICY REVIEW CYCLE.....	8
7 POLICY REFERENCES	8

070.110 Technology Acquisition	Current Version: 2.3
070.000 Administrative	Review Date: 02/19/2018

Policy Definitions

- **Acquisition:** an asset or object bought or obtained by CHFS.
- **Agency:** for the purpose of this document, agency or agencies refers to any department under the Cabinet of CHFS.
- **Confidential Data:** Defined by COT standards, is data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples would include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)

070.110 Technology Acquisition	Current Version: 2.3
070.000 Administrative	Review Date: 02/19/2018

070.110 Technology Acquisition

Category: 070.000 Administrative

1 Policy Overview

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through a technology acquisition policy. This document establishes the agency's Technology Acquisition Policy which helps manage risks and provides guidelines for security best practices regarding technology acquisition.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors or other defined groups/organizations providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

1.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and Office of the Secretary IT Executive. Senior Management supports the objective put into place by this policy. Violations may result in disciplinary action, which may include suspension, restricted access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

1.4 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted with OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking an exception to this policy.

1.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

070.110 Technology Acquisition	Current Version: 2.3
070.000 Administrative	Review Date: 02/19/2018

2 Roles and Responsibilities

2.1 Chief Information Security Officer (CISO)

This position is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This designated position is responsible to adhere to this policy.

2.2 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role along with the CHFS OATS Information Security (IS) Team is responsible for the adherence of this policy.

2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer

An attorney within CHFS Office of Legal Services (OLS) fills the Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer position. This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or CHFS OATS Information Security (IS) Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO, or CHFS OATS IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position is responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notifications in accordance with HIPAA rules and regulations.

2.4 CHFS Staff and Contract Employees

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

070.110 Technology Acquisition	Current Version: 2.3
070.000 Administrative	Review Date: 02/19/2018

3 Policy Requirements

3.1 Regulations

This policy establishes the framework for which all CHFS IT related procurements are to follow. All information technology purchases for CHFS must adhere to the Kentucky Finance and Administration Cabinet law and regulations for procurement. CHFS IT purchases adhere to the following Finance and Administration Cabinet law, regulation, and policy:

- Enterprise Architecture and Kentucky Information Technology Standards (KITS)- Information Technology Standards Committee (ITSC)
- Enterprise IT Process: COT-078 COT Cloud Stage Gate Process - The Cloud Stage Gate Process has been developed to review new projects that consider the use of cloud technology
- Kentucky Revised Statue (KRS) Chapter 45A- Kentucky Model Procurement Code
- Kentucky Administrative Regulations (KAR) 200- Chapter 5: Purchasing
- Finance and Administration Policies
- Finance and Administration Bid Protest Resources
- OATS Information Technology Standards

Additionally, all CHFS software development staff, vendors, and contractors are required to follow 065.014 CHFS Systems Development Lifecycle and New Application Development Policy.

3.2 Policy Violations

Individuals found to be in violation of this policy shall be subject to disciplinary actions that may result in, and not be limited to, suspension, termination, and may also be subject to criminal prosecution. Additional information can be found within the CHFS 020.308 Out-Processing/Termination of Information Technology Personnel Policy.

4 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

5 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

070.110 Technology Acquisition	Current Version: 2.3
070.000 Administrative	Review Date: 02/19/2018

6 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

7 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 020.308 Out-Processing/Termination of Information Technology Personnel Policy
- CHFS OATS Policy: 065.014 CHFS SDLC and New Application Development Policy
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS OATS Standards
- Enterprise Architecture and Kentucky Information Technology Standards (KITS)- Information Technology Standards Committee (ITSC)
- Enterprise IT Process: COT-078 COT Cloud Stage Gate Process
- Finance and Administration Bid Protest Procedure Resources
- Finance and Administration Cabinet- Manual of Policies and Procedures
- Internal Revenue Services (IRS) Publication 1075
- Kentucky Administrative Regulations (KAR) Title 200- Chapter 5: Purchasing
- Kentucky Revised Statutes (KRS) Chapter 040 Procurement activities- Distribution
- Kentucky Revised Statutes (KRS) Chapter 045A- Kentucky Model Procurement Code
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information